Lecture 10 - Polynomials in GF(2) and CRCs

Exercise 1: Write the addition, subtraction and multiplication tables for $GF(2)$. What logic function can be used to implement modulo-2 addition? Modulo-2 multiplication?

+	0	1
0	0	1
1	1	0

XOR

×	0	1
0	0	0
1	0	1

AND

Exercise 2: What are the possible results if we used values 0 and 1 but the regular definitions of addition and multiplication? Would this be a field?

+ results 0, 1, 2

× 0, 1

Exercise 3: What is the polynomial representation of the codeword 01101?

0 1 1 0 1

$0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0$

$+ x^2 + \quad + 1$

$x^3 \quad + x +$

Exercise 4: What is the result of multiplying $x^2 + 1$ by $x^3 + x$ if the coefficients are regular integers? If the coefficients are values in $GF(2)$?

$(x^2 + 1)(x^3 + x) = x^5 + x^3 + x^3 + x$

ordinary arithmetic: $= x^5 + 2x^3 + x$

GF(2) arithmetic $= x^5 + \cancel{0x^3} + x$

$x^5 + x$

Exercise 5: What is result of dividing $x^3 + x^2$ by $x^3 + x + 1$?

note: GF(2) subtraction = addition

$$\begin{array}{r|l} & \hspace{8em} 1 \\ \underbrace{1x^3 + 0x^2 + 1x + 1}_{G(x)} & \overbrace{1x^3 + 1x^2 + 0x + 0}^{M(x)} \\ & 1x^3 + 0x^2 + 1x + 1 \\ \hline & 0x^3 + 1x^2 + 1x + 1 \end{array}$$

$Q(x) = 1$

$R(x) = x^2 + x + 1$

Exercise 6: What is the probability that a randomly-chosen set of $n - k$ parity bits will match the correct parity bits for a given codeword? Assuming random data, what is the undetected error probability for a 16-bit CRC? For a 32-bit CRC?

k	n-k

$$\frac{1}{2^{n-k}}$$

$n-k = 16$

32

To compute CRC:

(1) append $n-k$ zeros (multiply $M(x)$ by x^{n-k})

(2) divide by $G(x)$

(3) the remainder is the CRC.

A CRC's generator polynomial is $\boxed{x^3 + 1}$. How many bits will the CRC have? Compute the CRC for the message sequence ~~1001~~ $\boxed{1010}$ using this generator polynomial.

$G(x) =$

$1x^3 + 0x^2 + 0x + 1x^0$

4 bits. in $G(x)$

3 bits in remainder & CRC

(1) append k−n bits to message

$M(x) = x^3 + 0x^2 + 1x^1 + 0x^0$ ___ ___ ___

by multiplying by x^3

$1x^6 + 0x^5 + 1x^4 + 0x^3 + \underline{0x^2} + \underline{0x} + \underline{0x^0}$

for convenience write only the coefficients: e.g. $G(x) =$ 1001

$G(x)$

```
1001 ) 1010.000
       1001
       ----
       0110
        1100
        1001
        ----
         1010
         1001
         ----
          011
```

$R(x)$, remainder CRC

we would transmit $M(x)$, $R(x)$

$\underbrace{1010}_{\text{data}}\ \underbrace{011}_{\text{CRC}}$

check:

```
1001 ) 1010011
       1001
       ----
       0110
        1101
        1001
        ----
         1001
         1001
         ----
            0
```

0 ✓ remainder is 0

∴ no errors.